UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/567,212	02/03/2006	Declan Patrick Kelly	NL030952	9660

24737 7590 10/14/2008

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
AVERY, JEREMIAH L	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/567,212	KELLY ET AL.	
	Examiner	Art Unit	
	JEREMIAH AVERY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 February 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-13 have been examined.

2. Response to Applicant's remarks has been given.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1, 3, 9, 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 6,009,116 to Bednarek et al., hereinafter Bednarek and further in view of United States Patent No. 6,438,235 to Sims, hereinafter Sims.

1. Regarding claim 1, Bednarek discloses a reproducing apparatus (1) for reproducing content stored in encrypted form on a record carrier (2), said record carrier (2) further storing a carrier region code (RCC) indicating in which region said content

shall be allowed to be reproduced and an encrypted region key (RK) for decrypting said content, said reproducing apparatus comprising:

a region code storage means (10) for storing a device region code (RCD) for use by a region code check unit (*Bednarek* – Figures 5, 9 and 10, column 5, lines 26-34, column 6, lines 20-26, column 12, lines 6-12, column 16, lines 1-10, column 17, lines 50-55, column 18, lines 2—33, column 19, lines 41-60, column 20, lines 64-67, column 21, lines 1-6 and column 22, lines 21-24 and 51-58),

a carrier region code reading means (12) for reading said carrier region code (RCC) from said record carrier (2) for use by said region code check unit (*Bednarek* – Figures 5, 9 and 10, column 4, lines 11-30, column 5, lines 26-34, column 6, lines 20-35, column 9, lines 57-67, column 10, lines 1-15, column 11, lines 30-41, column 12, lines 6-12, column 16, lines 1-10, column 17, lines 50-55, column 18, lines 3-33, column 19, lines 41-60, column 20, lines 64-67, column 21, lines 1-6 and column 22, lines 21-24 and 51-58),

said region code check unit (13) for checking if said carrier region code (RCC) matches said device region code (RCD) to determine if said record carrier is allowed to be reproduced by said reproducing apparatus (*Bednarek* – Figures 5, 7, 9-13 and 16, column 5, lines 26-34, column 6, lines 20-26, column 12, lines 6-23 and 56-65, column 16, lines 1-10, column 17, lines 50-67, column 18, lines 3-33, column 19, lines 41-60, column 20, lines 27-50 and 64-67, column 21, lines 1-6 and 25-36 and column 22, lines 21-24 and 51-58).

2. Bednarek significantly discloses the claimed invention, as cited above. However, Bednarek fails to disclose the limitations of "a device key storage means (11) for storing a device key (DK), said device key (DK) being different for all regions", "a region key reading means (14) for reading said encrypted region key (RK) from said record carrier (2) upon receiving an indication of a match between said device region code (RCD) and said carrier region code (RCC) from said region code check unit", "a region key decryption means (16) for decrypting said encrypted region key (RK) using said device key (DK) in case said carrier region code (RCC) matches said device region code (RCD)", "a content reading means (17) for reading said encrypted content from said record carrier (2)" and "a content decryption means (18) for decrypting said encrypted content using said decrypted region key and output means (19) for outputting said decrypted content". Sims discloses these limitations, as cited below.

3. Regarding claim 1, Sims discloses a device key storage means (11) for storing a device key (DK), said device key (DK) being different for all regions (column 4, lines 8-17, "each individual device, sets of associated devices, or manufacturers devices may utilize a different private key known only to these devices", column 12, lines 22-24, column 14, lines 40-53 and column 15, lines 23-31),

a region key reading means (14) for reading said encrypted region key (RK) from said record carrier (2) upon receiving an indication of a match between said device region code (RCD) and said carrier region code (RCC) from said region code check unit (column 11, lines 12-28, column 12, lines 22-24 and column 14, lines 25-39),

a region key decryption means (16) for decrypting said encrypted region key (RK) using said device key (DK) in case said carrier region code (RCC) matches said device region code (RCD) (column 19, lines 8-25, “the play-back device decrypts the XORed random and disk key utilizing the private media key),

a content reading means (17) for reading said encrypted content from said record carrier (2) (column 5, lines 8-13 and 16-20 and column 20, lines 16-32),

a content decryption means (18) for decrypting said encrypted content using said decrypted region key and output means (19) for outputting said decrypted content (column 7, lines 20-27, column 16, lines 41-56, “only this device may actually decrypt the content of media 100” and column 19, lines 43-58, “data packet is decrypted utilizing the private media key corresponding to the public media key stored on media 100”).

4. The motivation to combine would be “to provide protection in addition to the limited access of content through the use of cryptographic keys” (Sims – column 3, lines 25-27).

5. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Sims with the teachings of Bednarek in order “to obscure the content (information or data), using cryptographic methods, such that only a legitimate recipient can make use of that data, i.e., nobody but the content owner, or those authorized by him/her, is able to copy protected media content" (Sims - column 3, lines 35-45).

6. Regarding claim 3, Bednarek discloses wherein said carrier region code (RCC) comprises one or more tags (T), each tag (T) including a revocation information (P)

indicating regions from which record carriers are allowed for reproduction (column 4, lines 11-22 and 33-51, column 5, lines 19-25, column 6, lines 20-26, column 10, lines 16-29, column 21, lines 25-36 and column 22, lines 21-38 and 51-58).

7. Regarding claim 9, Bednarek discloses wherein said region code storage means (10), said device key storage means (11), said region code check unit (13) and said region key decryption means (16) are embedded in separate semiconductor device (100) (column 19, lines 41-60, "coordinate set might be securely stored in the Smart Card" and column 21, lines 2-6).

8. Regarding claim 11, Bednarek teaches a reproducing method for reproducing content stored in encrypted form on a record carrier (2), said record carrier (2) further storing a carrier region code (RCC) indicating in which region said content shall be allowed to be reproduced and an encrypted region key (RK) for decrypting said content, the method comprising the steps of:

reading said carrier region code (RCC) from said record carrier (2) (*Bednarek* – Figures 5, 9 and 10, column 4, lines 11-30, column 5, lines 26-34, column 6, lines 20-35, column 9, lines 57-67, column 10, lines 1-15, column 11, lines 30-41, column 12, lines 6-12, column 16, lines 1-10, column 17, lines 50-55, column 18, lines 3-33, column 19, lines 41-60, column 20, lines 64-67, column 21, lines 1-6 and column 22, lines 21-24 and 51-58),

checking if said carrier region code (RCC) matches a device region code (RCD) stored in a reproduction apparatus (1) (*Bednarek* – Figures 5, 7, 9-13 and 16, column 5, lines 26-34, column 6, lines 20-26, column 12, lines 6-23 and 56-65, column 16, lines 1-10,

column 17, lines 50-67, column 18, lines 3-33, column 19, lines 41-60, column 20, lines 27-50 and 64-67, column 21, lines 1-6 and 25-36 and column 22, lines 21-24 and 51-58).

9. Bednarek significantly teaches the claimed invention, as cited above. However, Bednarek fails to teach the claim limitations pertaining to "decrypting said encrypted region key (RK) using a device key (DK) stored in said reproduction apparatus (1) in case said carrier region code (RCC) matches said device region code (RCD)", "reading said encrypted content from said record carrier (2)" and "decrypting said encrypted content using said decrypted region key (RCD) and outputting said decrypted content". Sims teaches these limitations, as cited below.

10. Regarding claim 11, Sims teaches decrypting said encrypted region key (RK) using a device key (DK) stored in said reproduction apparatus (1) in case said carrier region code (RCC) matches said device region code (RCD) (column 19, lines 8-25, "the play-back device decrypts the XORed random and disk key utilizing the private media key),

reading said encrypted content from said record carrier (2) (column 5, lines 8-13 and 16-20 and column 20, lines 16-32),

decrypting said encrypted content using said decrypted region key (RCD) and outputting said decrypted content (column 7, lines 20-27, column 16, lines 41-56, "only this device may actually decrypt the content of media 100" and column 19, lines 43-58, "data packet is decrypted utilizing the private media key corresponding to the public media key stored on media 100").

11. The motivation to combine would be “to provide protection in addition to the limited access of content through the use of cryptographic keys” (Sims – column 3, lines 25-27).

12. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Sims with the teachings of Bednarek in order “to obscure the content (information or data), using cryptographic methods, such that only a legitimate recipient can make use of that data, i.e., nobody but the content owner, or those authorized by him/her, is able to copy protected media content" (Sims - column 3, lines 35-45).

13. Bednarek teaches the claimed invention, as cited above. However, Bednarek fails to teach the claim limitations pertaining to “a record carrier (2) for storing content in encrypted form for reproduction by a reproducing apparatus (1)”, “said record carrier (2) storing: i) said content in encrypted form, ii) a carrier region code (RCC) indicating in which region said content shall be allowed to be reproduced”. Sims teaches these limitations, as cited below.

14. Regarding claim 12, Sims teaches a record carrier (2) for storing content in encrypted form for reproduction by a reproducing apparatus (1) (column 11, lines 12-28, column 12, lines 22-24, column 14, lines 25-39 and column 20, lines 49-67, “the techniques of the present invention may be utilized with CD ROM formatted bulk storage devices with only simple differences as to where the secure area is hidden and how it was marked as not readable and how the disk key is hidden”),

said record carrier (2) storing:

i) said content in encrypted form (column 5, lines 8-13 and 16-20 and column 20, lines 16-32),

ii) a carrier region code (RCC) indicating in which region said content shall be allowed to be reproduced (column 11, lines 12-28, column 12, lines 22-24 and column 14, lines 25-39),

iii) an encrypted region key (RK) for decrypting said content, wherein during reproduction of said content by said reproducing apparatus said carrier region code (RCC) is used by said reproducing apparatus to determine if said carrier region code (RCC) matches a device region code (RCD) stored in a region code storage means of said reproduction apparatus (1) (column 7, lines 20-27, column 16, lines 41-56, "only this device may actually decrypt the content of media 100", and column 19, lines 43-58, "data packet is decrypted utilizing the private media key corresponding to the public media key stored on media 100"),

in case said carrier region code (RCC) matches said device region code (RCD) said encrypted region key (RK) is decrypted using a device key (DK) stored in a device key storage means of said reproduction apparatus (1) (column 19, lines 8-25, "the play-back device decrypts the XORed random and disk key utilizing the private media key),

said encrypted content is decrypted using said decrypted region key (RK) (column 7, lines 20-27, column 16, lines 41-56, "only this device may actually decrypt the content of media 100" and column 19, lines 43-58, "data packet is decrypted utilizing the private media key corresponding to the public media key stored on media 100").

15. The motivation to combine would be “to provide protection in addition to the limited access of content through the use of cryptographic keys” (Sims – column 3, lines 25-27).

16. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Sims with the teachings of Bednarek in order “to obscure the content (information or data), using cryptographic methods, such that only a legitimate recipient can make use of that data, i.e., nobody but the content owner, or those authorized by him/her, is able to copy protected media content" (Sims - column 3, lines 35-45).

17. Claims 2, 10 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bednarek and Sims, as applied to claims 1 and 11, respectively, above, and further in view of United States Patent No. 6,289,455 to Kocher et al., hereinafter Kocher.

18. Bednarek significantly discloses the claimed invention, as cited above. However, Bednarek fails to disclose the claim limitation pertaining to “wherein said region key decryption means (16) is adapted for decrypting said selected encrypted region key using said selected device key (DK)”. Sims discloses this, as cited below.

19. Regarding claim 2, Sims discloses wherein said region key decryption means (16) is adapted for decrypting said selected encrypted region key using said selected device key (DK) (column 19, lines 8-25, “the play-back device decrypts the XORed random and disk key utilizing the private media key).

20. The motivation to combine would be “to provide protection in addition to the limited access of content through the use of cryptographic keys” (Sims – column 3, lines 25-27).

21. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Sims with the teachings of Bednarek in order “to obscure the content (information or data), using cryptographic methods, such that only a legitimate recipient can make use of that data, i.e., nobody but the content owner, or those authorized by him/her, is able to copy protected media content" (Sims - column 3, lines 35-45).

22. Bednarek and Sims disclose the claimed invention, as cited below. However, they fails to disclose the claim limitations pertaining to " wherein said record carrier (2) stores at least two encrypted region keys (RK)", " wherein said device key storage means (11) is adapted for storing at least two device keys (DK) " and " wherein said reproducing apparatus (1) further comprises a key selection means (15) for selecting an encrypted region key (RK) from said at least two encrypted region keys and for selecting a device key (DK) from said at least two device keys using said carrier region code (RCC) and said device region code (RCD)". Kocher discloses these limitations, as cited below.

23. Regarding claim 2, Kocher discloses wherein said record carrier (2) stores at least two encrypted region keys (RK) (column 10, lines 36-67, “CryptoFirewall uses several keys, which are stored in protected memory 265 and loaded during

personalization", column 16, lines 47-67, column 17, lines 1-20, column 19, lines 51-67, column 20, lines 1-9, column 25, lines 5-13 and column 26, lines 25-40),
wherein said device key storage means (11) is adapted for storing at least two device keys (DK) (column 10, lines 35-47, column 16, lines 47-67 and column 26, lines 25-40),
wherein said reproducing apparatus (1) further comprises a key selection means (15) for selecting an encrypted region key (RK) from said at least two encrypted region keys and for selecting a device key (DK) from said at least two device keys using said carrier region code (RCC) and said device region code (RCD) (column 10, lines 36-67, "CryptoFirewall uses several keys, which are stored in protected memory 265 and loaded during personalization", column 16, lines 47-67, column 17, lines 1-20, column 19, lines 51-67, column 20, lines 1-9, column 25, lines 5-13 and column 26, lines 25-40).

24. The motivation to combine would be to "improve the security of systems used to distribute and protect digital content" (*Kocher* – column 5, lines 55 and 56).

25. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Kocher with the teachings of Bednarek and Sims in order to provide "a tamper-resistant device for regulating access to encoded digital content" (*Kocher* - column 5, lines 56-66).

26. Bednarek and Sims disclose the claimed invention, as cited above. However, they fail to disclose the claim limitation of claim 10 pertaining to "a counter (30) for counting the number of times the device region code (RCD) is changed and a reset means (31) for resetting the device region code (RCD) to a default value if a

predetermined number of changes has been made". Kocher discloses this, as cited below.

27. Regarding claim 10, Kocher discloses a counter (30) for counting the number of times the device region code (RCD) is changed and a reset means (31) for resetting the device region code (RCD) to a default value if a predetermined number of changes has been made (column 21, lines 22-33, column 27, lines 6-14 and 57-67 and column 28, lines 1-4).

28. The motivation to combine would be to "improve the security of systems used to distribute and protect digital content" (*Kocher* – column 5, lines 55 and 56).

29. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Kocher with the teachings of Bednarek and Sims in order to provide "a tamper-resistant device for regulating access to encoded digital content" (*Kocher* - column 5, lines 56-66).

30. Bednarek and Sims disclose the claimed invention, as cited above. However, they fail to disclose the claim limitation of claim 13 pertaining to "a computer program comprising program code means for causing a computer to perform the steps of the method as claimed in claim 11 when said computer program is executed on a computer". Kocher discloses this, as cited below.

31. Regarding claim 13, Kocher discloses a computer program comprising program code means for causing a computer to perform the steps of the method as claimed in claim 11 when said computer program is executed on a computer (column 4, lines 15-

27, “software includes instructions that implement and/or manage protocols and cryptographic keys involved in decrypting content”).

32. The motivation to combine would be to “improve the security of systems used to distribute and protect digital content” (*Kocher* – column 5, lines 55 and 56).

33. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Kocher with the teachings of Bednarek and Sims in order to provide "a tamper-resistant device for regulating access to encoded digital content" (*Kocher* - column 5, lines 56-66).

34. Claims 4-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bednarek and Sims as applied to claim 1 above, and further in view of United States Patent No. 5,907,655 to Oguro, hereinafter Oguro.

35. Bednarek and Sims significantly disclose the claimed invention, as cited above. However, they fail to significantly disclose the limitations found within claims 4-8. However, in combination with Oguro, said limitations are disclosed.

36. Regarding claim 4, Oguro discloses wherein said tags (T) are assigned to different nodes (N) of a tree structure representing all possible regions which are at least partly combined into region groups at a node (Figures 4 and 7, column 4, lines 14-39).

37. Regarding claim 5, Oguro discloses wherein said tree structure comprises at least two hierarchical layers (L0, L1) and wherein each node (N) has a number of branches, in particular three branches (Figures 4 and 7, column 4, lines 14-39 and column 5, lines 12-21).

38. Regarding claim 6, Oguro discloses wherein a number of device keys (DK) are assigned to each node (N), said number comprising at least one device key (DK) for each branch of said node (N) which is not assigned to all other branches of said node (N) (*Oguro* – Figures 4 and 7, column 4, lines 14-39).

39. Regarding claim 7, Oguro discloses wherein said device key storage means (11) are adapted for storing only device keys (DK) assigned to nodes (N) in the chain of the hierarchical tree from the top layer (L0) to the bottom layer (L2) (*Oguro* – Figures 4 and 7, column 4, lines 14-39).

40. Regarding claim 8, Oguro discloses wherein each tag (T) includes a termination information (E) indicating if there are further tags assigned to nodes of branches, branching off from the node to which said tag (T) is assigned, in lower hierarchical layers (column 4, lines 14-39, "Although Fig. 4 shows a two-layered structure, an additional lower layer may also be provided" and column 5, lines 12-21, "an additional lower layer becomes possible by data bit assignment").

41. The motivation to combine would be that "a disturbance flag for copy protection of the input picture signal is included in a pack for the auxiliary information and recorded in the auxiliary recording area" (*Oguro* – column 1, lines 52-66).

42. It would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Oguro within the method and apparatus of Bednarek and Sims in order to provide copy protection functionality within "a recording and reproducing method and apparatus for digital video signals" (*Oguro* – column 1, lines 42-49).

Response to Arguments

43. Applicant's arguments with respect to claims 1-13 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

44. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

45. The following United States Patents are cited to further show the state of the art with respect to the protection of digital content, such as:

United States Patent No. 6,640,305 to Kocher et al., which is cited to show a digital content protection method and apparatus.

United States Patent No. 6,304,658 to Kocher et al., which is cited to show a leak-resistant cryptographic method and apparatus.

United States Patent No. 7,003,671 to Kusakabe, et al., which is cited to show an information processing device and method.

United States Patent No. 5,915,254 to Reece et al., which is cited to show a mobile communication service provider selection system.

United States Patent No. 7,058,414 to Rofheart et al., which is cited to show a method and system for enabling device functions based on distance information.

United States Patent No. 5,815,661 to Gosling, which is cited to show a platform independent object and object application loader and method.

United States Patent No. 6,446,209 to Kern et al., which is cited to show a storage controller conditioning host access to stored data according to security key stored in host-inaccessible metadata.

46. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

47. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

48. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431

/Christopher A. Revak/

Primary Examiner, Art Unit 2431